

Manuscript version: Author's Accepted Manuscript

The version presented in WRAP is the author's accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:

<http://wrap.warwick.ac.uk/116547>

How to cite:

Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.

ATHENA: A Pagerank-based Scheme to Solve the Thundering Herd in Authentication

Chao Chen¹, Sang Woo Lee², Tim Watson¹, Carsten Maple¹, and Yi Lu¹

¹Cyber Security Centre, University of Warwick, United Kingdom

²ETRI, Electronics and Telecommunications Research Institute, South Korea

¹{c.chen.27, tw, cm, y.lu.16}@warwick.ac.uk, ²ttomlee@etri.re.kr

Abstract—Vehicles in intelligent transport systems (ITS) react to an emergency situation by broadcasting critical messages like Decentralized Environmental Notification Messages (DENMs). A digital signature is attached to each message to secure the integrity of communication, and this message is inoperative until the authentication completes. This creates a challenge for vehicles to verify massive messages in some scenarios where it could incur the thundering herd in authentication, if there is a critical situation happening in heavy road traffic. To address this problem, we propose ATHENA, a pagerank-based scheme to solve the thundering herd in ITS authentication that utilises the transmission of messages and pagerank algorithm to rank the broadcasting vehicles. Simulation results show the efficiency of ATHENA and the effectiveness of performance enhancements compared with others.

Index Terms—ITS, Authentication, Security;

I. INTRODUCTION

ITS plays a vital role in the future traffic system, for it can fundamentally enhance the safety and efficiency of the road traffic. Vehicles and road side units (RSUs) equipped with multiple sensors (like 3-D lidar, radar, stereo camera and laser) can effectively detect their surrounding environment [1] [2]. Additionally, the equipped on-board units (OBUs) with multiple type of network interface (e.g., DSRC, Wifi and cellular) support them to communicate with others promotely by constantly broadcasting messages [3], which facilitates vehicles and RSUs to extend their capabilities beyond the non-line-of-sight (NLOS). Due to the importance of the exchanging messages, they are an easy target for malicious attackers [4]. Therefore, authentication is a core procedure for message communication. Each message has attached an additional digital signature to guarantee the intactness and security, and each participant, vehicle or RSU, cannot access this message until the verification of messages has completed.

In order to achieve road safety within ITS, ETSI has recommended Elliptic Curve Digital Signature Algorithm (ECDSA) to generate the signature and verify these signatures [5]. Each vehicle will react and broadcast at most 10 DENMs per second to others [6], if this vehicle detects a critical situation. Consequently, there are thousands of DENMs to be verified per second, creating a form of the well-known “thundering herd” problem. In Fig 1, a road hazard happens in a highway roundabout with the heavy traffic at the central area, all surrounding vehicles and RSUs equipped with sensors

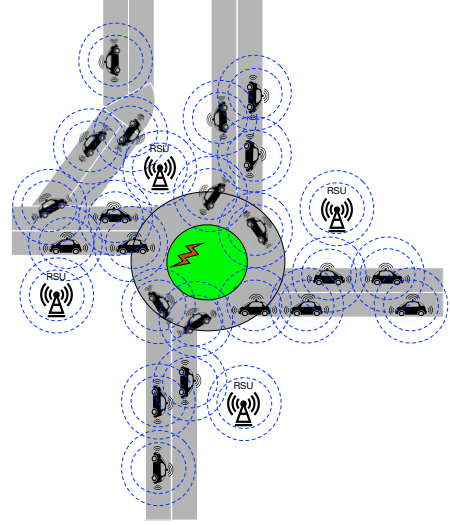


Fig. 1: The exemplar of thundering herd in ITS

detect this and immediately broadcast DENMs to others, and other vehicles also will verify and broadcast these messages once they have been notified. To explore the authentication cost in details, we have evaluated the signature and verification in ECDSA-256 from the ETSI standards at different hardware configurations (OBU ARM v7, Intel i3 and i5) in the Table I.

Hardware	ECDSA_sign (ms)	ECDSA_verify (ms)
OBU-ARMv7	27.9	33.7
Intel-i3	10.2	14.6
Intel-i5	5.46	7.32

TABLE I: The comparisons of ECDSA on different hardware

Furthermore, we have measured the loss ratio due to a slow verification compared to the required requirements (10 DENM per second). In Fig 2-(1), with the increasing number of vehicles, the loss ratios of verification become more noticeable in three configurations. For the OBU and Intel-i3, for example, the loss ratio reaches around 50% if there are more than 15 vehicles, which is gradually getting higher with increasing vehicles. Despite some queueing approaches [7] [8] to queue the received messages for 100 ms can mitigate this as in Fig 2-(2), it cannot change the fact that total time cost for verifying

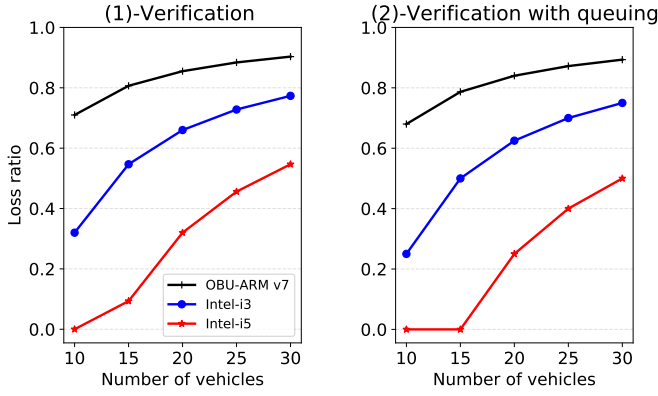


Fig. 2: The loss ratio of authentication messages

all messages is still constant and the improvement of loss ratio is not that significant for the overall. Additionally, when the thundering herd happens, other messages, like Cooperative Awareness Messages (CAMs), are being jammed and become more difficult to received and processed by vehicles.

In the rest of this paper, we propose a new pagerank-based authentication scheme, ATHENA, to address this problem. Section II describes the comparison of other approaches and the motivation of pagerank algorithm, and we present the overview of ATHENA in Section III. The evaluated results are discussed in Section IV and the conclusion is in Section V.

II. RELATED WORK

A number of schemes have been proposed to reduce verification processing overhead [5], [7]–[9]. They are mainly based on the queuing approach as a buffer where received messages can be prioritised or scheduled by a predefined order. [5] chooses a random order for the verification to reduce the congestion, whilst [9] [8] prioritise the verification based on the distance between transmitter and receiver. Although [7] adopts the Markov model to adjust the order of verification based on critical situations amongst different physical areas, the overall verification time cost for all messages is still unchanged as we mentioned in Section I. Massive broadcast is inevitably happening in the real world traffic, authentication solely relying on the queueing is incapable of processing the thundering herd problem and it causes unnecessary accidents.

[10] proposed the pagerank algorithm as a powerful tool to rank web pages in the Internet. It constructs each web page as a vertex in a directed graph, and the hyper-links point into a web page as incoming edges, whilst the hyper-links that point from a web page to other web page are represented as outgoing edges. The rank of a web page thus can be inferred from these incoming and outgoing edges. The value of a rank is determined by its linked web pages and the initial quality of itself, then iteratively computes it by the Eq 1, where N is the number of web pages, $E_{in}(p_i)$ is the number of incoming edges for web page p_i , $E_{out}(p_j)$ is the number of outgoing edges for web page p_j . There are $E_{in}(p_i)(p_i = p_1, p_2, \dots, p_{E_{in}})$ edges that point out to web page p_i from other pages. $PR(p_i)$

represents the page rank value for p_j and the initial quality of a web page is the initial PR value, which is defined as $\frac{1}{N}$. The damping factor is denoted as d , which is usually recommended as 0.85 to make sure the iteration is convergent.

$$PR(p_i) = \frac{1-d}{N} + d \sum_{E_{in}(p_i)} \frac{PR(p_j)}{E_{out}(p_j)} \quad (1)$$

III. AN OVERVIEW OF ATHENA

A. Standardised messages in the thundering herd

ETSI defines the emergency messages as DENM [6]. A signed DENM contains the basic information for message timestamps, payload data and the digital signature, etc. The payload data, which is the core element for a DENM, is comprised of four containers for different aspects.

The *situation container* and the *location container* are the two key containers for ATHENA. The former container records the type of the detected event and the information quality, which is generated at the application level and it ranges from 7 as the highest to 1, the lowest of information quality regarding to the accuracy of a detecting event. The latter has the information of event location as a trace, which refers to a set of consecutive path point positions leading to the event position. Other two containers, the *management container* and the *a la carte container* have the basic management information related to DENM management and validity of duration or other specific information have not included in other containers. We implemented our proposed protocol in the negation flag from the *management container*, which has the highest priority level that can stop broadcasting DENMs.

B. ATHENA protocol

Signed DENMs are received, verified and forwarded amongst vehicles, and they will arrive at the closest RSU, eventually. The proposed ATHENA at RSU then constructs the communication graph based on the set of point positions in all its received messages from the *location container*, this communication graph is applied for the pagerank algorithm to determine the top rank of vehicles to generate DENMs.

Protocol 1 ATHENA at vehicle side

```

1: procedure BROADCASTING
2:   while DENM signal == True do
3:     while negation flag  $\neq$  True do
4:       for  $m_i \in \vec{M}_i$  do
5:         a score of information quality to  $m_i$ 
6:         ECDSA_sign( $m_i$ )
7:         signed  $\vec{M}_i$  broadcast to neighbours.
8:       no more DENMs are generated or broadcasted.
```

As we displayed in Protocol 1 for the vehicle side, once a vehicle detects the emergency signal to generate DENMs, it will go to check its negation flag. If the negation flag is not true, this vehicle will generate 10 DENMs per second that each one of them has a score of information quality regarding to

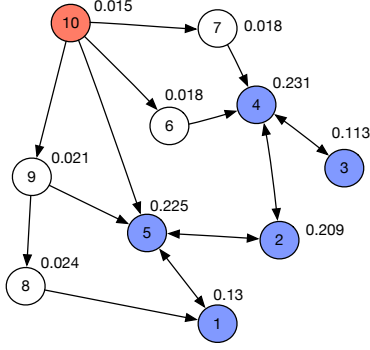


Fig. 3: The graph of DENMs communication

this situation to be broadcasting. For these generated DENMs, a digital signature generated by ECDSA will be assigned to broadcast from line 4 to 7. Otherwise, if this vehicle received the notification of negation flag with its unique id, which will immediately stop the vehicle to generate DENMs. This vehicle then only receives or forward incoming DENMs, because RSU has determined another suitable vehicles to broadcast DENMs.

Next, we define ATHENA protocol at RSU side. Since the RSU constantly receives messages from its surrounding vehicles, once the number of received messages per second has reached a predefined threshold, which can dynamically be adjusted based on the capability of verification. It will trigger ATHENA protocol at RSU side to build the communication graph, G , for all received messages. Then we can compute the highest rank vehicles by Eq 1. And this message will broadcast the unique id of selected high ranking vehicles and the negation flag to all other vehicles to execute Protocol 1.

C. Pagerank for the broadcasting vehicles

Pagerank algorithm is to measure the importance of broadcasting vehicles based on their connections. The most widely used approach to represent the connection relationships is the graph model, and the graph is built as $G = (V, E)$ where V is the vertices set and E is the edge set. Consequently, vehicles or RSUs are represented by vertices, and the path of transmitted DENMs amongst vehicles are denoted as edges.

When DENMs finally arrived at a vehicle or a RSU from an “eyewitness” vehicle, they already have been transmitted and forwarded by a path of other vehicles at different positions, which is recorded by the trace in the *location container*. This is analogous to the hyper-link pointing to a web page from another web page, the received vehicle has a trace path pointing to the original sending vehicle. Like the blue vertices 1 to 5 in Fig 3, they are 5 original eyewitness vehicles to broadcast DENMs to their neighbours. The rest of vertices, as the rest of vehicles received and forwarded the emergency information from those original eyewitnesses. For example, the edge from vertex 8 to vertex 1, indicates the transmission of emergency messages to vehicles 8 is received from vehicle 1. The red vertex 10 represents the RSU that can construct this communication graph based on the *location container* from all received DENMs. Therefore, the number of “eyewitness”

vehicles (blue vertices) starting to broadcast DENMs are analogous to the potential web pages to be ranked, and the task of finding the highest ranking “eyewitness” vehicles to broadcast thus is equal to find the top ranking web pages from all web pages. After this graph is built, we can apply Eq. 1 by [11] to calculate the relative ranking value for each vertex as shown in Fig 3 and broadcast the top ranking vehicles to rest of vehicles. The time complexity of pagerank algorithm is $O(n + E)$, where n is the number of vertices and E is the number of edges.

IV. PERFORMANCE EVALUATION

A. Simulation Setup

We developed the simulation model to analyse the efficiency and effectiveness of ATHENA. This simulation is used for the transmission and verification of signed messages amongst vehicles. Each vehicle generates 10 signed messages per second based on ETSI standards. We have evaluated ECDSA-256 algorithm to sign and verify a secured message based on Table I. In the realistic scenario, specialised hardware security module or trusted platform module are adopted to improve the cryptographic operations by using higher CPU rather than directly using OBU [12]. For generality, we choose Intel-i3 as our specialized hardware security module for signing and verifying.

To simulate the thundering herd, we choose the roundabout scenario as shown in Fig 1. Assuming there are 100 vehicles and RSUs randomly distributed in this roundabout and a percentage of vehicles are the first eyewitnesses detecting an emergency to broadcast DENMs.

B. The comparison of ATHENA with the Oracle

We first evaluate the differences between the information quality by adopting a few of highest ranking vehicles and the information quality of top ranking of vehicles to the Oracle, which we regard as the ideal, where a vehicle has 7, the highest information quality.

We ran the simulation by 500 times, and a random communication graph amongst all connecting elements is generated at each experiment. Then, we evaluated an increasing percentage of vehicles as the first eyewitnesses broadcast to represent the differences between top ranking vehicles and the Oracle in the Fig 4. The lower part of the main box represents the 25-percentile, the upper part is 75-percentile, and the orange line is the median. The lower whisker is the 5-percentile, and the upper one is the 95-percentile, and the green bullet is the mean for 500 simulations. It is reasonable that the more top ranking vehicles broadcast DENMs, the higher information quality can achieve, the less information quality differences compared to the Oracle. When we choose top 10 highest ranking vehicles to broadcast, the differences are already zero, so we have not listed the results of rank beyond 10. However, we can see the results from top 3 ranking appear to be remarkably close at all three different percentages of eyewitnesses. 75 percentile, median and mean differences are less than 1, and 5 and 25 percentile of differences are zero, which means no information

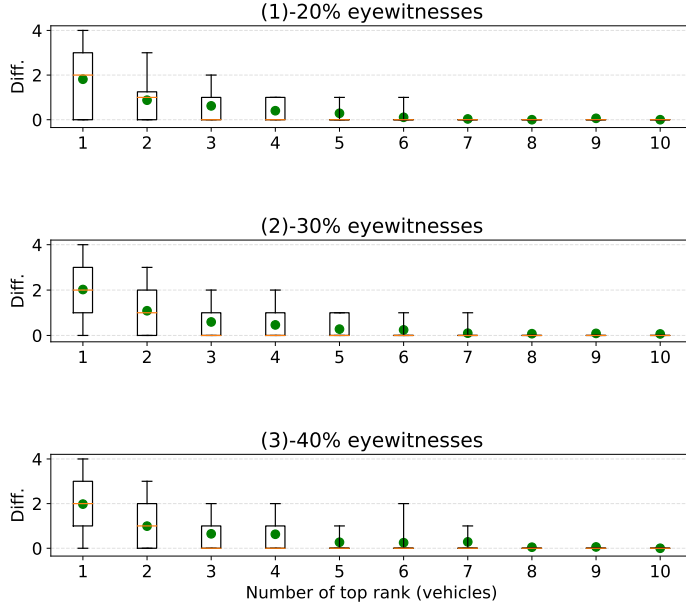


Fig. 4: The comparison of top rank with the Oracle

quality loss between the Oracle and it is empirically the best choice.

C. The performance improvements achieved by ATHENA

The experiments in this subsection investigate the performance improvements achieved by ATHENA in different fields. Due to the results that we represented in Fig 2, the loss ratio of verification is considerably growing with the increasing number of vehicles. On the another hand, ATHENA is capable of having more vehicles broadcasting without any loss ratio. This is because ATHENA tames the thundering herd for only the highest 3 vehicles broadcasting, which is totally acceptable for most scenarios.

Therefore, in Fig 5, we displayed the number of duplicate messages have been reduced by ATHENA choosing top ranking 3 from 10 seconds to 5 minutes. The longer broadcast lasts, the more duplicate messages have been reduced, which explains the significant saving from the verification on the vehicles side.

V. CONCLUSION

We have described a pagerank-based scheme to solve the thundering herd problem in ITS authentication. ATHENA utilises the path of locations to convert it as a graph model, and we use the pagerank algorithm to determine the highest rank vehicles to broadcast. We have evaluated the results of a few number of highest ranking vehicles are almost identical to the results of all vehicles in the same scenario to broadcast, and it improves the loss ratio of verification and shows a large number of verified messages have been reduced.

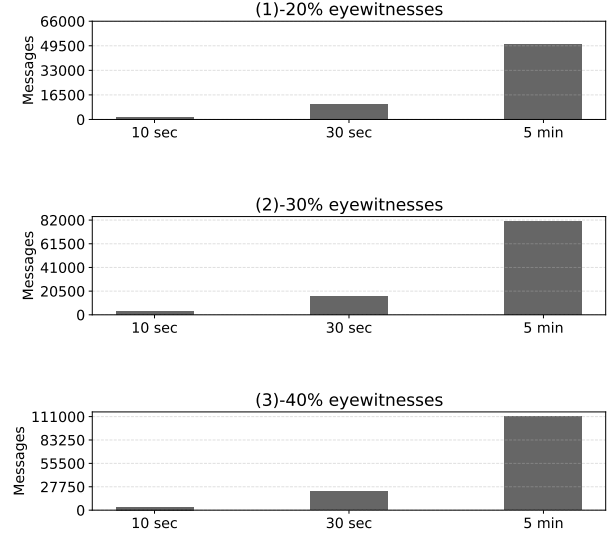


Fig. 5: The number of reduced messages

ACKNOWLEDGEMENT

This work is conducted under international technology R&D collaboration program which is supported by the Ministry of Trade, Industry & Energy (MOTIE) and Korea Institute for Advancement of Technology (KIAT) (N0001710).

REFERENCES

- [1] A. Geiger, M. Lauer, Benjamin, H. Rapp, C. Stiller, and J. Ziegler, "Team annieway's entry to the 2011 grand cooperative driving challenge," *IEEE Transactions on Intelligent Transportation Systems*, 2012.
- [2] P. Newman, G. Sibley, M. Smith, M. Cummins, A. Harrison, C. Mei, I. Posner, R. Shade, D. Schroeter, L. Murphy *et al.*, "Navigating, recognizing and describing urban spaces with vision and lasers," *The International Journal of Robotics Research*, 2009.
- [3] T. Higuchi and O. Altintas, "Interface selection in hybrid v2v communications: A hierarchical approach," in *Vehicular Networking Conference (VNC)*. IEEE, 2017.
- [4] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intelligent Transportation Systems*, 2015.
- [5] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Communications*, vol. 13, no. 5, 2006.
- [6] ETSI. (2014) Intelligent transport systems (its); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service. [Online]. Available: <http://v.ht/u9TE>
- [7] C. Chen, S. W. Lee, T. Watson, C. Maple, and Y. Lu, "Caesar: A criticality-aware ecdsa signature verification scheme with markov model," in *Vehicular Networking Conference (VNC)*. IEEE, 2017.
- [8] E. B. Hamida and M. A. Javed, "Channel-aware ecdsa signature verification of basic safety messages with k-means clustering in vanets," in *AINA*. IEEE, 2016.
- [9] Z. Li and C. Chigan, "On resource-aware message verification in vanets," in *Communications (ICC)*. IEEE, 2010.
- [10] L. Page, S. Brin, R. Motwani, and T. Winograd, "The pagerank citation ranking: Bringing order to the web." Stanford InfoLab, Tech. Rep., 1999.
- [11] A. Hagberg, P. Swart, and D. S. Chult, "Exploring network structure, dynamics, and function using networkx," Los Alamos National Lab.(LANL), Los Alamos, NM (United States), Tech. Rep., 2008.
- [12] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *International Conference on Information Security and Cryptology*. Springer, 2011, pp. 302–318.